



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 15 septembre 2005
N° CERTA-2005-AVI-347

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des équipements Lynksys

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-347>

Gestion du document

Référence	CERTA-2005-AVI-347
Titre	Vulnérabilité des équipements Lynksys
Date de la première version	15 septembre 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité iDEFENSE du 13 septembre 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Lynksys WRT54G Wireless-G Broadband Router.

3 Résumé

De nombreuses vulnérabilités découvertes dans certains équipements Lynksys permettent à un utilisateur mal intentionné de porter atteinte à l'intégrité des données, de contourner la politique de sécurité ou de provoquer un déni de service.

4 Description

Cinq vulnérabilités ont été découvertes dans le micro-programme embarqué dans l'équipement. Celles-ci permettent à un utilisateur ayant accès au réseau local de contourner la politique de sécurité afin :

- de modifier arbitrairement les fichiers de configuration du routeur ;
- de provoquer un déni de service du serveur web interne.

5 Solution

Se référer aux bulletins de sécurité et/ou sur le site Internet du constructeur (cf. section Documentation).

6 Documentation

- Site Internet "Linksys" :
<http://www.linksys.com>
- Bulletin de sécurité iDEFENSE #304 du 13 septembre 2005 :
<http://www.odefense.com/application/poi/display?id=304&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #305 du 13 septembre 2005 :
<http://www.odefense.com/application/poi/display?id=305&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #306 du 13 septembre 2005 :
<http://www.odefense.com/application/poi/display?id=306&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #307 du 13 septembre 2005 :
<http://www.odefense.com/application/poi/display?id=307&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #308 du 13 septembre 2005 :
<http://www.odefense.com/application/poi/display?id=308&type=vulnerabilities>
- Référence CVE CAN-2005-2799 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2799>

Gestion détaillée du document

15 septembre 2005 version initiale.